Administrator Services

This section covers the following topics:

- Access to Administrator Services
- Set General Options
- Set Library and User Defaults
- Default User Profiles
- Set PF-Keys
- Logon/Countersign Error Processing
- Logon Records Processing
- Definition of System Libraries
- Processing of Maintenance Log Records
- Definition of System File Access

The Administrator Services subsystem provides several functions which apply to the Natural Security system as a whole and to all security profiles.

You select "Administrator Services" on the Main Menu. If you have access to the subsystem (see Access to Administrator Services below), the Administrator Services Menu will be displayed.

The Administrator Services Menu consists of two screens. With PF7 and PF8, you can switch between the two screens. They provide the following functions:

Administrator Services Menu 1:

- Set General Options (*)
- Set Library and User Defaults (*)
- Default User Profiles (*)
- Set PF-Keys (*)
- Logon/Countersign Error Processing
- Logon Records Processing
- Interface Subprograms
- Definition of System Libraries

Administrator Services Menu 2:

- Processing of Maintenance Log Records
- Definition of Utility Defaults/Templates
- Definition of System File Access

You should study the functions marked above with (*) before you start defining objects to Natural Security. The other Administrator Services functions are not directly related to defining objects to Natural Security.

Access to Administrator Services

As far as access to the Administrator Services subsystem is concerned, the following applies:

- If owners are specified in the security profile of the Natural Security library SYSSEC, only these owners have access to the Administrator Services subsystem.
- If SYSSEC has no owners assigned, every ADMINISTRATOR may access the Administrator Services subsystem.

For information on owners in library security profiles, see the sections Library Maintenance and Countersignatures.

Set General Options

Before you start defining objects to Natural Security, it is advisable to specify a number of options which will apply to the Natural Security system as a whole.

On the Main Menu, you select "Administrator Services". The Administrator Services Menu will be displayed.

> **Note:**
> Access to Administrator Services may be restricted; see Access to Administrator Services above.

On the Administrator Services Menu, you select "Set general options". The Set General Options screen will be displayed, which provides the following options:

- Transition Period Logon
- Activate Security for Development Server File
- Maximum Number of Logon Attempts
- Suppress Display of Logon Messages
- Lock User Option
- User Password History
- Free Access to Functions via Interface Subprograms
- Minimum Number of Co-Owners
- Deletion of Non-Empty Libraries Allowed
- Overwriting of Defaults Possible
- Display DBID/FNR of FSEC
- Exit Functions with Confirmation
- Logging of Maintenance Functions

The individual options are described below.

Transition Period Logon

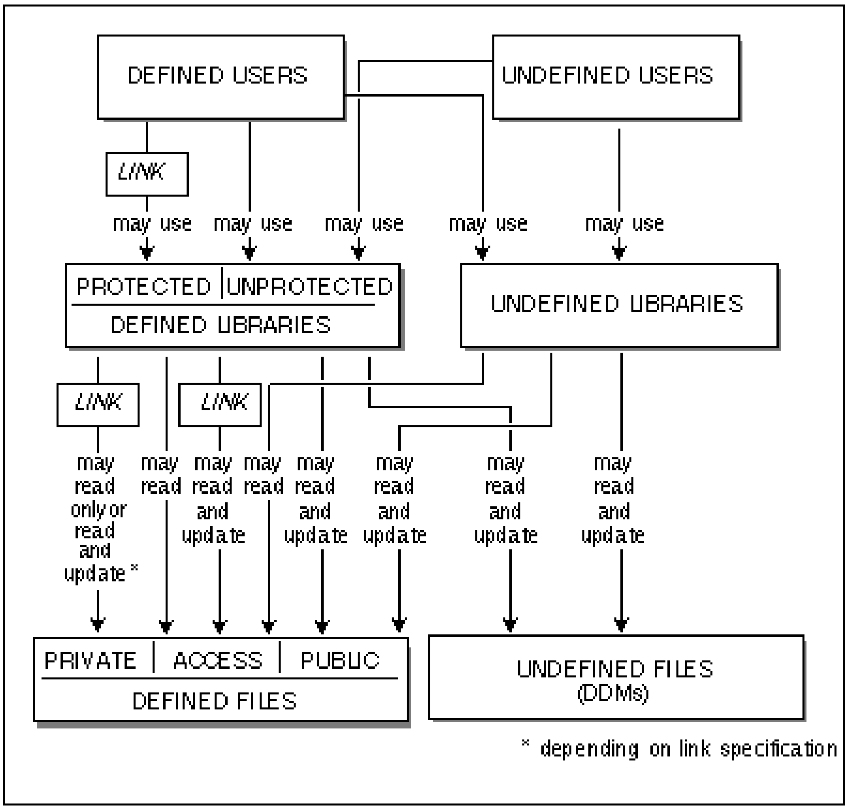
This option allows a smooth transition from an unprotected Natural environment to one protected by Natural Security.

Y	• Users not yet defined to Natural Security may log on to libraries which are not yet defined to Natural Security or which are defined as unprotected. • Libraries not yet defined to Natural Security may be accessed by any (defined or undefined) user. • Undefined libraries may access DDMs which are not yet defined to Natural Security as well as files of status PUBLIC and ACCESS. • Undefined DDMs may be accessed by any (defined or undefined) library.
N	Only users defined to Natural Security may use Natural. Any library not defined to Natural Security cannot be used.

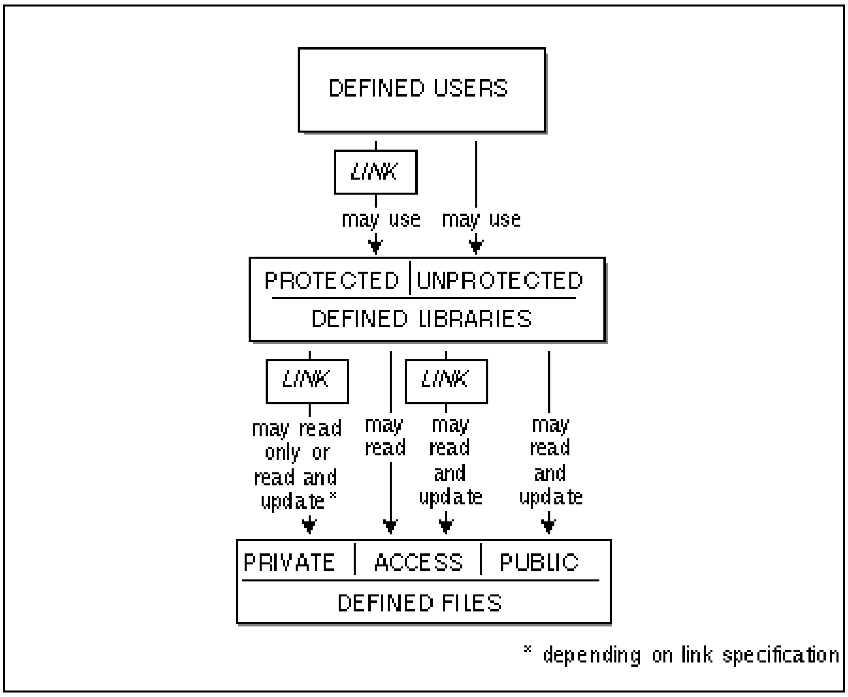
The effects of the Transition Period Logon settings are illustrated below.

If you have had an unprotected Natural installation and Natural Security is now being installed, it is advisable to set the Transition Period Logon to "Y" so as to ensure that work with Natural may continue while users and libraries are defined to Natural Security. Once all objects and links are defined, the Transition Period Logon should be set to "N".

Conditions of use under Transition Period Logon = Y:



Conditions of use under Transition Period Logon = N:



Activate Security for Development Server File

This option only appears if the Natural Development Server is installed and the current Natural session uses a development server file. It is only relevant if you wish to control the access to base and compound applications on the development server file. For details, see the section Protecting Natural Development Server Applications.

Y	Security for the development server file is active: The application security profiles for base and compound application defined in Natural Security take effect and control the access to the Natural Development Server objects "base applications" and "compound applications" on the development server file. The FSEC system file which is being used when this option is set to "Y" will be defined to the development server file. This development server file can then only be used in a Natural Security environment. All security checks made by the Natural Development Server in the Natural Studio’s application workspace will be performed using the security definitions on that FSEC system file. If you set this option to "Y", this will also activate Predict Security (if not already activated in Predict, by setting the Predict parameter "Protect Predict File" on the General Defaults > Protection screen to "Y"). Please note that the activation of Predict Security will not only affect the access to base and compound applications, but may also cause other Predict Security settings not related to applications to take effect. The database ID and file number of the development server file for which the option is activated will be shown on the Set General Options screen.
N	Security for the development server file is not active. Application security profiles are not evaluated.

Maximum Number of Logon Attempts

1-5	You may specify how many attempts to log on users shall have. After *n* unsuccessful logon attempts, the logon procedure will be terminated, the user "thrown out", and a logon-error record written (for information on logon-error records, see Logon Errors below).

Suppress Display of Logon Messages

This option may be used to suppress the display of the messages NAT0853 and NAT0854, which indicate that a logon to a library has been successful. By default, one of these messages is displayed after every successful logon to a library.

Y	Messages NAT0853 and NAT0854 will not be displayed.
N	Messages NAT0853 and NAT0854 will be displayed.

Lock User Option

This option may be used to prevent users from trying to misuse other users’ user IDs and passwords. This applies to the logon procedure (see Logon Procedure in the section Logging On) and to the countersignatures feature (see the section Countersignatures).

Y	For logon attempts, the following applies: Once a user has reached the maximum number of logon attempts without entering the correct password, the respective user will be locked, i.e. the user ID made invalid. Not only will all Natural Security user IDs that were tried out be locked, but also the user’s operating-system login name (as identified by the Natural system variable *INIT-USER), if that is used as a user ID for a Natural Security user profile. For countersign attempts, the following applies: After too many invalid passwords (the maximum number of logon attempts also applies here) on a Countersign screen, the user who invoked the respective function (as identified by his/her Natural Security user ID) will be locked.
F	The same as "Y"; in addition, the Natural session is terminated when the user is locked.
N	The Lock User feature is not active.

User Password History

This option may be used to exercise more control over the users' usage of passwords to enforce more efficient password protection.

Y	Password history is active. This has the following effects: ● The last *nnn* passwords used by each user are recorded by Natural Security. These last *nnn* passwords cannot be used again by the user as new password. You set the number of passwords to be recorded in the window displayed when you activate this option. ● A user is forced to change his/her password at logon when the password has been changed by an administrator in the user's security profile. ● You can define certain rules to which passwords must conform. You define these password rules by using the function "Set Library and User Defaults" (see below).
N	Password history is not active.

Other password-related Natural Security features are:

- the minimum password length, which can be set on the "Set Library and User Defaults" screen (see below),
- and the password expiration (field "Change after *nnn* days"), which can be set in user security profiles (see the section User Maintenance).

Free Access to Functions via Interface Subprograms

You may specify who may access Natural Security maintenance and retrieval functions from outside Natural Security via the interface subprograms provided. For details on these subprograms, see the section Interface Subprograms.

Y	Maintenance and retrieval functions may be accessed from outside Natural Security via the interface subprograms by anybody who may use the subprograms. If you set this option to "Y", you can protect each maintenance/retrieval function separately using functional security (see the section Functional Security).
R	Retrieval functions (but not maintenance functions) may be accessed from outside Natural Security via the interface subprograms by anybody who may use the subprograms. If you set this option to "R", you can protect each retrieval function separately using functional security (see the section Functional Security).
N	Maintenance and retrieval functions may be accessed from outside Natural Security only by users (of type ADMINISTRATOR) who may also use the Natural Security library SYSSEC. With the subprograms, they may only perform those functions they are also allowed to perform within SYSSEC, and only under the same conditions under which they may perform them in SYSSEC.

Maintenance functions are all functions of the subprograms NSCFI, NSCLI, NSCOB and NSCUS - except their Display functions.

Retrieval functions are all functions of the subprograms NSCCHCK, NSCDEF, NSCDU, and NSCXR and of the subprograms whose names begin with "NSCDA", as well as the Display functions of the subprograms NSCFI, NSCLI, NSCOB and NSCUS.

Minimum Number of Co-Owners

0-3	You may specify the minimum number of co-owners for each owner of a security profile. The number set here will be valid for all security profiles and cannot be modified individually.

For an explanation of co-owners, see the section Countersignatures; leave the value set to "0" until you have read that section.

Deletion of Non-Empty Libraries Allowed

You may specify whether a library’s (or private library’s) security profile can be deleted if the library contains any source or object modules.

Y	A library’s security profile can be deleted even if the library contains any source or object modules. When you try to delete a library profile, Natural Security will issue a warning if the library is not empty. This option only affects the deletion of a library’s *security profile*; the Natural library itself and the modules it contains are not deleted.
N	A library’s security profile cannot be deleted as long as the library itself still contains any source or object modules.

Overwriting of Defaults Possible

You may specify whether the defaults set on the Set Library And User Defaults screen may be overwritten in individual security profiles.

Y	The default settings specified on the Set Library And User Defaults screen may be overwritten in the individual security profiles.
N	The default settings specified on the Set Library And User Defaults screen may not be overwritten in any security profile. They will be valid for all libraries/users without exception.

Library and user defaults are described under Set Library and User Defaults below.

Display DBID/FNR of FSEC

You may specify whether the database ID and file number of the current Natural Security system file (FSEC) are to be displayed on the menu and selection screens within the library SYSSEC.

Y	The database ID and file number of the current Natural Security system file (FSEC) will be displayed on the menu and selection screens within the library SYSSEC. They will be displayed in the top right-hand corner below the current date.
N	The database ID and file number of the FSEC file will not be displayed in SYSSEC.

Exit Functions with Confirmation

You may specify how you wish Natural Security to react when you leave a function by pressing PF2, PF3, PF12 or PF15.

Y	Each time you leave a function in Natural Security by pressing PF2, PF3, PF12 or PF15, a window will be displayed in which you have to specify whether the modifications you made before pressing the key are to be saved or not or whether you wish to return to the function.
N	When you leave a function by pressing PF2, PF3 or PF15, the modifications you made before pressing the key will be saved. When you leave a function by pressing PF12, the modifications you made before pressing the key will *not* be saved.

For details on which function is assigned to which key, see the section Set PF-Keys below.

Logging of Maintenance Functions

This option allows you to ascertain who has modified which security profiles and administrator services settings.

Y	Log records are written for modifications to security profiles and administrator services settings.
N	Modifications are not logged.

When you set this option to "Y", a window will be displayed in which you can specify the following:

Log file DBID/FNR	The database ID and file number of the file in which the log records are to be stored. This file must have been loaded during the installation process of Natural Security. **Note:** Once "Logging of Maintenance Functions" has been activated, you cannot change the log file assignment. You have to deactivate the option, before you can assign another database ID or file number.
Logging even if no actual modification	**Y** - Modifications are also logged if nothing has actually been changed; that is, if a security profile or administrator services setting has been invoked for modification, but no actual change has been made to the profile/setting. **N** - Modifications are only logged if a profile/setting has actually been changed.
Logging of changes to	You mark with "Y" the object types whose modifications are to be logged: ● administrator services settings, ● user security profiles, ● library security profiles, ● file security profiles, ● application security profiles, ● mailbox security profiles, ● various types of external object security profiles. "Administrator services settings" in this context means all functions listed on the Administrator Services Menu (except "Interface Subprograms"). **Note:** Modifications to utility security profiles are not logged separately. Instead, default profiles and templates are handled under administrator services settings, library-specific utility profiles under library security profiles, and user-specific and user-library specific utility profiles under user security profiles.

To change the above specifications once you have activated the writing of log records, you press PF4 on the Set General Options screen.

To view the log records, you use the function "Processing of Maintenance Log Records" (see below).

Set Library and User Defaults

Before you start defining users and libraries to Natural Security, it is advisable to specify a number of default settings. These default settings will then apply to all library security profiles or user security profiles respectively.

On the Main Menu, you select "Administrator Services". The Administrator Services Menu will be displayed.

> **Note:**
> Access to Administrator Services may be restricted; see Access to Administrator Services above.

On the Administrator Services Menu, you select "Set library and user defaults". The Set Library And User Defaults screen will be displayed, which provides the following options:

Library Defaults:

- Active cross-reference for Predict
- Logon recorded
- Natural programming mode
- Restart
- Maintenance with Natural utilities
- Clear source area by logon
- Execute startup transaction in batch
- Steplibs

User Defaults:

- ETID
- Minimum password length
- Private library for administrator/person

The above library and user default items also appear on the security profile screens of libraries and users respectively, where you may specify them for each user/library individually. The values you specify for these items on the Set Library And User Defaults screen will appear as defaults on the security profile screen of each object (if applicable). If the general option "Overwriting of defaults possible" (see above) is set to "Y", you may overwrite the defaults in the individual security profiles.

Library Defaults

Active Cross-Reference for Predict

You may specify whether an active cross-reference in Predict (if installed) will be generated for a library.

Y	An active cross-reference in Predict will be generated.
N	An active cross-reference in Predict will not be generated.
F	An active cross-reference in Predict will be forced.
D	Objects to be cataloged must be documented in Predict (however, no active cross-reference will be generated).

See the Predict documentation for details on active cross-references.

Logon Recorded

Y	Every time a user logs on to a library, a logon record will be written by Natural Security. You may review the activities of users by viewing these records with the "Logon Records Processing" function. For details on logon records, see Logon Records Processing below.
N	Logons to libraries will not be recorded.

Note:
If the general option "Transition Period Logon" (see above) is set to "Y" , a logon record will also be written every time an undefined user logs on, and every time a user logs on to an undefined library.

Natural Programming Mode

R	Reporting mode.
S	Structured mode.

Restart

You may specify whether during the logon procedure an Adabas OPEN command with or without End of Transaction ID (ETID) is to be executed.

Y	During the logon procedure an OPEN command with ETID will be executed.
N	During the logon procedure an OPEN command without ETID will be executed.

Maintenance with Natural Utilities

This setting only applies to the old Version 2 utility protection mechanism described in the section System Libraries And Utilities - Old Protection Mechanism. As explained in the section Protecting Natural Utilities, *it is strongly recommended that this old mechanism no longer be used*.

N	The contents of a library are *not protected* against being maintained with Natural utilities.
O	The contents of a library may be maintained with Natural utilities only by *owners* of the library's security profile.
P	The contents of a library may be maintained with Natural utilities under *protection rules*, that is, only by users who may log on to the library under Natural Security.

This applies the Natural utilities NATLOAD, NATUNLD, SYSERR and SYSMAIN, and to the Natural system command SCAN. For details see the section System Libraries And Utilities - Old Protection Mechanism.

Clear Source Area by Logon

Y	The editor's source work area will be cleared automatically when a user logs on from the library to another.
N	The editor's source work area remains as it is when a user logs on from the library to another.

Execute Startup Transaction in Batch

Y	The startup transaction specified in a library security profile will also be executed (once) in batch mode.
S	The startup transaction specified in a library security profile will also be executed in batch mode; in addition, its name will be placed in the Natural system variable *STARTUP.
N	If the NEXT/MORE line is allowed for a library, the startup transaction specified in the library security profile will not be executed in batch mode. If the NEXT/MORE line is not allowed, the startup transaction will also be executed (once) in batch mode.

See also the section Natural Security In Batch Mode.

Steplibs

You may enter the names of the libraries which are to be the steplib libraries (concatenated libraries) for a library. If a library does not contain a requested programming object, the steplibs will be searched for the object one after another in the order in which they are specified.

You can specify the name of the first steplib in the Steplibs field on the Set Library And User Defaults screen. To specify more than one steplib, enter an asterisk (*) in the field or press PF4: a window will be displayed, in which you can specify up to 9 default steplibs.

User Defaults

ETID

You may specify which values are to be used as IDs for End of Transaction data (ETIDs).

G	ETIDs will be generated by Natural Security.
U	The ID by which a user is defined to Natural Security, i.e. the value of the Natural system variable *USER, will be used as ETID. If the Automatic Logon feature (which is described in the section Logging On) is used, the value of *USER will be identical to that of *INIT-USER.
I	The value of the Natural system variable *INIT-USER will be used as ETID.
T	The value of the Natural system variable *INIT-ID will be used as ETID.
N	ETIDs will not be used.

If you do not remember the possible values you may specify, enter a question mark (?) or an asterisk (*) in the field: a window will be displayed; in the window, mark the desired value with a character or with the cursor; the value will then be written into the ETID field.

See the Natural Reference documentation for details on the above-mentioned system variables.

Minimum Password Length

1-8	A user password must not consist of fewer characters than the number specified here. When you set this length, please bear in mind that by default passwords are identical to user IDs (see the section User Maintenance).

Private Library for Administrator/Person

You may specify whether users of type PERSON or ADMINISTRATOR may have a personal ("private") library.

Y	PERSONs and ADMINISTRATORs may have a private library.
N	PERSONs and ADMINISTRATORs may not have a private library.

For information on private libraries, see the section Private Libraries.

Password Rules

This option can only be used if the general option "User Password History" (see above) is active.

It allows you to define rules to which user passwords must conform. When you press PF5 on the "Set Library and User Defaults" screen, a window is displayed in which you can define the following:

Password mask	You can define a "mask" to which passwords must conform; that is, you can define for each position in a password whether it has to be an alphabetical character (A) or a number (N) or whether it can be either (*). For example, "***AAA" means that the first three characters can be either numbers or letters, while the second three have to be letters. The length of the mask must correspond to the user default "Minimum Password Length" (see above).
Each character only once	If this value is set to "Y", passwords must not contain a character twice. For example, "THIRST" would not be allowed, because it contains two T’s.
Disallow double characters	If this value is set to "Y", passwords must not contain double characters. For example, "LITTLE" would not be allowed, because of the double T.
Check password for pattern	If this value is set to "Y", a password must not be the same as the current value of the Natural system variable *USER. Moreover, a new password must not be too similar to the old one: a new password will be rejected if its last three characters are identical to those of the old password.

In addition, the window displays the maximum number of stored passwords, that is, the number of passwords recorded by Natural Security for each user which cannot be used again by the user as new password.

Default User Profiles

Before you use default user security profiles, you should be familiar with the "normal" way of defining users as explained in the section User Maintenance.

When you add new users, you can either type in every item of every user security profile by hand, or you can use a pre-defined default user profile for the creation of a user security profile. When you have to define numerous users whose security profiles are to be very similar to one another, you can define in a default profile the items which are to be the same for many users, and then use this default profile as the basis for the individual security profiles. By using default user profiles, you can thus reduce the amount of work required to define users to Natural Security.

You create a default profile as described below, and then use it as the basis for a user security profile as described in the section User Maintenance.

How to Create a Default Profile

On the Main Menu, enter code "A" for "Administrator Services". The Administrator Services Menu will be displayed.

Note:
Access to Administrator Services may be restricted; see Access to Administrator Services above.

On the Administrator Services Menu, enter code"U" for "Default user profiles". The Default User Profiles selection list will be displayed.

In the command line of this screen, enter the command "ADD". The Add Default User Profile window will be displayed.

In this window, enter the following:

- the *user ID* of the default profile,
- the *user type* of the default profile.

For information on user IDs and user types, see the section User Maintenance.

The Add Default User Profile screen will be displayed. On this screen you may define a default user profile.

The Add Default User Profile screen corresponds more or less to the Add User screen for the same user type. The individual items you may define as part of a user profile are described under Components of a User Profile in the section User Maintenance. Please note, however, that you can define some items only in an individual security profile, but not in a default profile.

Default profiles are maintained like individual user profiles (as described in the section User Maintenance).

How to Use a Default Profile

When you add a new user, you can specify the ID of a default profile which is to be used as the basis of the user security profile you are creating.

The *user type* of the default profile must be the same as that of the security profile you use it for.

When you use a default profile to add a new user, the following items are copied from the default profile into the user profile:

- the default library,
- the password change interval,
- the language indicator,
- the time differential,
- the activation dates,
- the batch user ID,
- the mailboxes,
- the security notes,
- the "Logon recorded" setting,
- the session options.

When you use a default profile to add a new user, the user ID, the user name and the owners are *not* copied from the default profile into the user profile.

On the Add User screen, you can then overwrite the items copied into the user profile and specify further items.

Note:
To define numerous users who are to have identical security profiles, you can also use the "Multiple Add User" function (which is described in the section User Maintenance).

Set PF-Keys

On the Main Menu, you select "Administrator Services". The Administrator Services Menu will be displayed.

> **Note:**
> Access to Administrator Services may be restricted; see Access to Administrator Services above.

On the Administrator Services Menu, you select "Set PF-keys". The Set PF-Keys screen will be displayed.

On this screen, you may assign functions and names to keys, as described below.

Functions may be assigned to certain keys only. Names may be assigned to all keys.

PF-Key Functions

The functions assigned to the following PF-keys cannot be modified:

Key	**Function**	**Explanation**
PF01	Help	For each Natural Security screen there is a Help Info which provides an explanation of the screen and tells you how to proceed. If you press PF1 on any Natural Security screen, the appropriate Help Info will be displayed.
PF02	Previous Menu	This key returns you to the menu screen from which you have invoked the current processing level. By default, the modifications you made before leaving a function with PF2 will be saved; see also the general option "Exit Functions with Confirmation" above.
PF03	Exit	This key causes a given processing level to be terminated and the screen of the next higher processing level to be displayed. By default, the modifications you made before leaving a function with PF3 will be saved; see also the general option "Exit Functions with Confirmation" above.
PF04	Additional Options	When you are on a security profile screen, you can press this key (instead of marking the Additional Options field on the screen with "Y") to display the Additional Options selection window for a security profile.
PF05		Various, different functions on different screens (as described where appropriate).
PF06	Flip	The PF-key lines at the bottom of the Natural Security display either PF-keys 1 to 12 or PF-keys 13 to 24. By pressing PF6, you can switch from one display to the other.
PF07	Previous Page (-)	This key scrolls a displayed list one page backward.
PF08	Next Page (+)	This key scrolls a displayed list one page forward.
PF12	Cancel	This key causes a given processing level to be terminated and the screen of the next higher processing level to be displayed. By default, the modifications you made before leaving a function with PF12 will *not* be saved; see also the general option "Exit Functions with Confirmation" above.
PF13	Refresh	This key undoes all modifications you have made on a screen but which have not yet been saved. The fields on the screen will be reset to the values they had before you changed them.
PF14		(reserved for future use)
PF15	Menu	This key invokes the Natural Security Main Menu. By default, the modifications you made before leaving a function with PF15 will be saved; see also the option "Exit Functions with Confirmation" above.
PF16 to PF18		(reserved for future use)
PF19	First Page (- -)	This key scrolls a displayed list to its beginning.
PF20 to PF24		(reserved for future use)

Note:
CLR has the same function as PF12.

PF09, PF10, PF11, PA1, PA2

You may assign a function to each of these keys yourself. The function assigned will then be invoked within Natural Security by pressing the appropriate PF-key (or PA-key).

One of the following functions may be assigned to a PF-key (or PA-key):

- a Natural system command,
- a Natural terminal command,
- a Natural program.

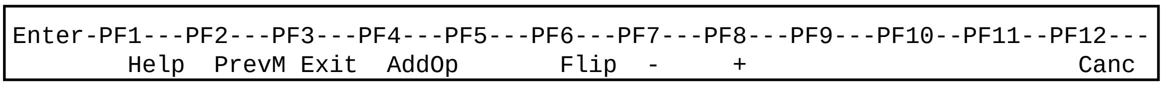
For information on the available system commands and terminal commands, see the Natural Reference documentation.

To assign a function to a key, you enter a command or program name in the "Function" column of the Set PF-Keys screen next to a key number.

PF-Key Names

You may name all PF-keys (including those whose function assignments you cannot change). The names may be up to 5 characters long and can be entered in the "Name" column of the Set PF-Keys screen.

The assigned names will appear in the PF-key lines which are displayed at the bottom of each Natural Security screen:



```
Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
        Help  PrevM Exit  AddOp       Flip  -     +                       Canc
```

If no name is displayed for a PF-key, this indicates that the function assigned to this key is not applicable to the screen displayed.

The lines display either PF-keys 1 to 12 or PF-keys 13 to 24. By pressing PF6, you can switch from one display to the other.

Logon/Countersign Error Processing

The Logon/Countersign Error Processing functions serve two purposes:

- The Logon Error Processing functions are used to view unsuccessful attempts to log on to Natural.
- The List/Unlock Locked Users function, which is only used in conjunction with the "Lock User Option", is used to view (and unlock) users who have been "locked" due to logon or countersign errors.

Logon Errors

Note:
Logon Error Processing is independent from and has nothing to do with the Logon Records Processing function (which is described below); do not confuse one with the other.

On the Set General Options screen, you can specify the "Maximum number of logon attempts" (see above) by entering a number *n* in the range from 1 to 5 (the default is 5). Every time a user makes *n* consecutive unsuccessful logon attempts, the user will be "thrown out" and a *logon error record* will be written by Natural Security. The logon error record contains detailed information on each of the *n* logon attempts that led to the record being written (for example, which user and library IDs were entered by the user). The records may be viewed by using the Logon Error Processing functions.

Being able to view logon error records serves the following purposes:

- You can ascertain whether unauthorized people have tried to gain access to Natural.
- You can ascertain what users do wrong when they try to log on. Users may then be informed how to log on correctly.
- You can ascertain whether users have been given the appropriate access rights. A user may, for example, try to log on to an library he/she is not (but should be) allowed to use. In this case you may then make the necessary Natural Security maintenance adjustments to the security profiles and relationships concerned.

The recording by Natural Security of logon errors cannot be "switched off".

Locked Users

If the "Lock User Option" (see Set General Options above) is active, users may be "locked" due to logon or countersign errors:

- **Logon errors:** Once a user has reached the maximum number of logon attempts without entering the correct password, the user will be locked.
- **Countersign errors:** After entering too many invalid passwords on the Countersignature screen, the user who invoked the function requiring the countersignatures will be locked. (For information on countersignatures, see the section Countersignatures.)

With the function "List/Unlock Locked Users" you may see which users have been "locked" due to logon or countersign errors. You may also unlock them again.

If the "Lock User Option" is not active, countersign errors are not recorded, whereas logon errors are always recorded (as explained above) regardless of the "Lock User Option".

How to Invoke Logon/Countersign Error Processing

On the Main Menu, you select "Administrator Services". The Administrator Services Menu will be displayed.

> **Note:**
> Access to Administrator Services may be restricted; see Access to Administrator Services above.

On the Administrator Services Menu, you select "Logon/countersign error processing". The Logon/Countersign Error Processing Menu will be displayed, which provides the following functions:

- List error entries
- Delete error entries
- Display individual error entries
- List/unlock locked users

The individual functions are described below.

When you select one of these functions, you can also specify the following options on the Logon/Countersign Error Processing Menu:

Order of Records *	**T** - The logon error records will be in order of terminal IDs, as defined by the Natural system variable *INIT-ID. **P** - The logon error records will be in order of user IDs, as defined by the Natural system variable *INIT-USER.
Start Value	If you do not wish to get all, but only a certain range of logon error records or locked users respectively, you may specify a start value as described in the section Finding Your Way In Natural Security.

* This option has no impact on the List/Unlock Locked Users function.

List Error Entries

This function displays a list of logon error records.

The list can be scrolled as described in the section Finding Your Way In Natural Security.

To select one error entry from the list to have a closer look at it, you type in the corresponding sequential number (first column of the list) in the "Enter no. to be processed" field. A screen displaying the "Error History" of the selected error will be invoked (this display is the same as for the Display Individual Error Entries function).

Delete Error Entries

This function displays a list of logon error records, similar to that displayed by the List Error Entries function (see above).

The list can be scrolled as described in the section Finding Your Way In Natural Security.

- If you wish to delete all error entries displayed, press ENTER.
- If you do not wish to delete all error entries displayed, press PF3 to return to the Logon/Countersign Error Processing Menu.
  If you wish to delete individual error entries, use the Display Individual Error Entries function.

It is recommended that logon error records be deleted periodically so as to save space on the FSEC system file.

See also the direct command ERRDEL below.

Display Individual Error Entries

This function displays the "Error History" of logon error entries one by one.

List/Unlock Locked Users

This function is only applicable if the "Lock User Option" (which is described under Set General Options above) is active. It will display a list of those users whose security profiles have been "locked" due to logon or countersign errors. The list will be in alphabetical order of user IDs. On the list you may then unlock individual users.

When you invoke the List/Unlock Locked Users function, the List Locked Users screen will be displayed.

The list can be scrolled as described in the section Finding Your Way In Natural Security.

The column "T" of the List Locked Users screen indicates the type of error which caused the user to be locked:

C	Countersign error
L	Logon error

In the case of a countersign error, the ID of the owner whose password was entered incorrectly and the ID of the object the locked user attempted to modify will be displayed next to the type.

In the case of a logon error, the error numbers will be displayed next to the type.

To select one entry from the list, you enter the corresponding sequential number (first column of the list) in the "Enter no. to be processed" field. A window will be displayed.

- If you wish to unlock the user, enter a "Y" in the window.
- If you do not wish to unlock the user, leave the "N" already entered in the window unchanged.

Note:
You may also unlock a locked user by modifying his/her security profile (as described in the section User Maintenance).

Deleting All Error Entries - Direct Command ERRDEL

With the Delete Error Entries function (described above), you can delete logon/countersign error entries page by page.

However, if you wish to delete *all* logon/countersign error entries at once, you enter the direct command ERRDEL in the command line.

Logon Records Processing

This function allows you to see which users have been using which libraries.

On the Set Library And User Defaults screen you may specify the library default "Logon recorded" (see Set Library and User Defaults above). Also, you may specify the option "Logon recorded" in the security profile of each library (and private library) and each user (see the sections Library Maintenance and User Maintenance respectively).

A logon record will be written by Natural Security:

- every time a user logs on to a library (or private library) in whose security profile the "Logon recorded" option is set to "Y";
- every time a user in whose security profile the "Logon recorded" option is set to "Y" logs on to any library.

If the general option"Transition Period Logon" (see above) is set to "Y", a logon record will also be written every time an undefined user logs on (regardless of the setting of the option "Logon recorded"), and every time a user logs on to an undefined library.

You may view these logon records by using the function "Logon records processing".

How to Invoke Logon Records Processing

On the Main Menu, you select "Administrator Services". The Administrator Services Menu will be displayed.

> **Note:**
> Access to Administrator Services may be restricted; see Access to Administrator Services above.

On the Administrator Services Menu, you select "Logon records processing". The Logon Records Processing Menu will be displayed, which provides the following functions.

Functions of Logon Records Processing

Each of these functions displays a list of logon records.

Function	Explanation
List Logon Records	With this function, you may view a list of logon records - and have the option to delete individual logon record entries.
Delete Logon Records	With this function, you may view a list of logon records - and have the option to delete whole pages of logon record entries.
Delete Logon Records But Last	With this function, you may view a list of logon records - and have the option to delete whole pages of logon record entries except the latest entry for each user ID (that is, the latest entry for each user ID will not be deleted).

When you select one of the above functions, you can specify the following selection options on the Logon Records Processing Menu:

Order of Records	**U** The logon records will be listed in alphabetical order of user IDs. **L** The logon records will be listed in alphabetical order of library IDs. **UX** Same as "U", but listing only logon records of undefined users. **LX** Same as "L", but listing only logon records to undefined libraries.
Start Value	If you do not wish to view a list of all logon records, but would like only certain logon records to be listed, you may specify a start value as described in the section Finding Your Way In Natural Security.
Date from/to Time from/to	If you wish to view only records of logon that occurred in a specific period of time, you may specify a period of time in these fields.

The Start Value and Date/Time options may be combined.

The Date/Time options only apply to the functions List Logon Records and Delete Logon Records; for the function Delete Logon Records But Last, they are ignored.

Deleting All Logon Records - Direct Command LOGDEL

With the above Delete functions, you can delete logon records page by page.

However, if you wish to delete *all* logon records at once, you enter the direct command LOGDEL in the command line.

Definition of System Libraries

This function is used as part of the installation procedure for an initial installation of Natural Security. It allows you to automatically create library security profiles for system libraries (that is, libraries whose names begin with "SYS") of Natural and its subproducts.

If you use this function, you have to set the Natural profile parameter MADIO to a value of at least "2000".

Do not apply this function to SYS libraries containing Natural utilities, as it is recommended that utilities be protected as described in the section Protecting Natural Utilities.

On the Main Menu, you select "Administrator Services". The Administrator Services Menu will be displayed.

Note:
Access to Administrator Services may be restricted; see Access to Administrator Services above.

On the Administrator Services Menu, you select "Definition of system libraries".

A list of the system libraries of Natural and all Natural subproducts installed at your site will be displayed. For each system library, a library-specific security profile is provided in which all the necessary components are already defined appropriately.

On the list, you can either mark with "AD" individual libraries to which you wish their pre-defined profiles to be applied one by one, or you can choose to have the pre-defined profiles applied to all product system libraries simultaneously by marking the corresponding product with "AD".

For further information, see the Natural Security installation description in your Natural Installation Guide.

Processing of Maintenance Log Records

This function can only be used if the general option "Logging of Maintenance Functions" has been activated. If this option has been activated, *log records* are written when security profiles and administrator services settings are modified. The writing of log records allows you to ascertain who has modified which security profiles and administrator services settings.

To view the log records, you use the function "Processing of maintenance log records".

On the Main Menu, you select "Administrator Services". The Administrator Services Menu will be displayed.

> **Note:**
> Access to Administrator Services may be restricted; see Access to Administrator Services above.

On the Administrator Services Menu 2, you select "Processing of maintenance log records". A menu will be displayed, from which you can select the following functions:

- Display Status of Logging Function
- List Administrator Services Maintenance Logs
- List Security Profile Maintenance Logs
- Log File Maintenance
- List Last Logon Records

Display Status of Logging Function

This function displays the following information:

- for which types of objects log records are written,
- the number of log records that have been written for each type of object,
- whether the option "Logging even if no actual modification" is set or not.

Note:
For this function, the fields "Object Type", "Start Value" and "Date from/to" on the menu have no effect.

List Administrator Services Maintenance Logs

This function displays a list of the log records that have been written for modifications to administrator services settings.

The log records are listed in chronological order.

On the list, the following information is displayed for each log record: the Administrator Services function performed, the ID of the user who made the modification, and the date and time of the modification.

On the list, you can mark a log record with any character: the screen on which the modification was made will then be displayed; on that screen, fields whose values were changed are displayed intensified.

By default, the "Date from/to" fields on the menu both contain the current date; that is, only the log records written today are listed. To list older log records, you change the date values on the menu as desired before you invoke this function.

Note:
For this function, the fields "Object Type" and "Start Value" on the menu have no effect.

List Security Profile Maintenance Logs

This function displays the log records that have been written for modifications to security profiles.

In the "Object type" field, you specify the type of object (USer, LIbrary, etc.) whose modified security profiles you wish to be listed. If you leave the field blank or enter a question mark (?), a window will be displayed in which you can select the desired object type. If you enter an asterisk (*), all log records for all security profiles will be listed.

In the "Start value" field, you can enter an object ID as start value for the list to be displayed.

By default, the "Date from/to" fields on the menu both contain the current date; that is, only the log records written today are listed. To list older log records, you change the date values on the menu as desired before you invoke this function.

The log records are listed in chronological order.

On the list, the following information is displayed for each log record: the function performed on the security profile, the ID of the security profile, the ID of the user who made the modification, and the date and time of the modification.

On the list, you can mark a log record with any character: the security profile in which the modification was made will then be displayed. If you press PF2 on the security profile screen, the fields whose values were changed will be displayed intensified (and, if applicable, a message will indicate whether an actual modification was made or not).

Log File Maintenance

On mainframes, this function can only be used in batch mode.

This function allows you to write/read the contents of the log file to/from a work file.

Log records have to be written to a work file when the log file becomes full. Thus, the work file serves as an "archive" for the log records.

The work files to be used are Work File 1 and Work File 5. On OpenVMS, UNIX and Windows, Work File 5 must be a file with the extension ".sag".

The output reports will be written to the print files CMPRT01 and CMPRT02.

When you invoke this function, you will be prompted to specify the database ID and file number of the log file. If you later wish to specify another log file, you press PF5 on the Log File Maintenance menu.

When you invoke this function, the Log File Maintenance menu is displayed, from which you can select the following functions:

Code	Function	Explanation
LI	**List Log Records**	This function is used to list the contents of the log file. The output contains the same information as displayed by the function List Security Profile Maintenance Logs: a list of all modified profiles/settings, as well as every profile concerned (indicating the profile components which were modified). The output consists of two reports: ● the "List of History Log Entries" report will be written to print file CMPRT01, ● the "Detail History Log Entries" report will be written to print file CMPRT02.
WR	**Write Log Records to Work File**	This function is used to write log records from the log file to Work File 5 (without deleting them from the log file).
WD	**Write Log Records to Work File and Delete**	This function is used to write log records from the log file to Work File 5, and delete them from the log file.
RA	**Read Log Records from Work File**	This function is used to read log records from Work File 5 onto the log file.
SA	**Scan Work File**	This function is used to scan the contents of Work File 5.

The Log File Maintenance function can also be invoked with the direct command LOGFILE.

Possible object types to be entered on the Log File Maintenance menu are:

*****	all
AD	administration functions
AA	all (base and compound) applications
AB	base applications
AC	compound applications
DD or **FI**	DDMs/files
LI	libraries
MA	mailboxes
US	users

For object-type codes of external objects, see Types of External Objects.

Other parameters that can be specified on the Log File Maintenance menu are:

Start value	You can specify a start for the objects to be written/read.
Date from/to	If you wish to process only log records that were created in a specific period of time, you may specify a range of dates in these fields.
Work File 1	The name of Work File 1.
Work File 5	The name of Work File 5.

Example:

To write log records from the log file to Work File 5, the CMSYNIN batch input file would contain the following commands:

```
LOGFILE
FIN
```

The CMOBJIN batch input file might contain the following specifications:

```
SYSSEC,DBA,PASSWORD
22,241
WR,US,,2001-07-01,2001-07-25
```

The first line must contain the library ID "SYSSEC" and the user ID and password of the respective Natural Security ADMINISTRATOR.

The second line must contain the database ID and file number of the log file from which the records are read.

The third line must contain the function code and object type (possible values are the same as on the Log File Maintenance menu) - optionally followed by various parameters (whose sequence and possible values correspond to those of the corresponding fields on the Log File Maintenance menu).

When you scan or read the work file, you have to specify the following parameter in the JCL:

```
 WORK=((5),OPEN=ACC)
```

Sample Batch Job 1 for Mainframes - Writing Log Records to Work File:

```
//DBA       JOB DBA,CLASS=K,MSGCLASS=X
//**
//** WRITE LOGGING OF MAINTENANCE DATA TO WORK FILE 5
//** DELETE RECORDS FROM LOG FILE
//**

//NSCnnBAT EXEC PGM=NATBATnn,REGION=2400K,
// PARM=('IM=D,FNAT=(22,210),INTENS=1,FSEC=(22,240),',
//       'MT=0,MAXCL=0,MADIO=0,AUTO=OFF,WORK=((5),OPEN=ACC)')
//STEPLIB DD   DSN=PRODNAT.LOAD,DISP=SHR
//DDCARD   DD  DISP=SHR,DSN=PRD.NATnn.JOBS(ADADB22)
//CMPRINT  DD  SYSOUT=X
//CMWKF05   DD DSN=NSC.LOG.WKF05,
//    DISP=(NEW,CATLG),DCB=(RECFM=VB,LRECL=4624,BLKSIZE=4628),
//    SPACE=(TRK,(5,2))
//CMSYNIN   DD *
SYSSEC,DBA,password
LOGFILE
22,241
WD,US,,2001-07-01,2001-07-25
.
FIN
/*
//*
```

In the above example, the log records of all user security profiles modified between 1st and 25th July 2001 are written to Work File 5, and are then deleted from the log file.

Sample Batch Job 2 for Mainframes - Writing Log Record Reports to Printers:

```
//DBA       JOB DBA,CLASS=K,MSGCLASS=X
//**
//** LIST LOG RECORDS-WRITE REPORTS OF MAINTENANCE DATA TO PRINTER
//**
//NSCnnBAT EXEC PGM=NATBATnn,REGION=2400K,
// PARM=('IM=D,FNAT=(22,210),INTENS=1,FSEC=(22,240),',
//       'MT=0,MAXCL=0,MADIO=0,AUTO=OFF')
//STEPLIB  DD  DSN=PRODNAT.LOAD,DISP=SHR
//DDCARD   DD  DISP=SHR,DSN=PRD.NATnn.JOBS(ADADB22)
//** CMWKF01   DD DISP=SHR,DSN=NSC.LOG.WKF01
//** CMWKF05   DD DISP=SHR,DSN=NSC.LOG.WKF05
//CMPRINT  DD SYSOUT=X
//CMPRT01  DD SYSOUT=X
//CMPRT02  DD SYSOUT=X
//CMSYNIN  DD *
LOGFILE
FIN
/*
//CMOBJIN  DD *
SYSSEC,DBA,password
22,241
LI,AD,,2001-06-06,2001-06-06
LI,US,MILL*,2001-05-01,2001-05-31
.
/*
//*
```

In the above example, the log records of all administrator services settings modified on 6th June 2001 and of all user security profiles modified in May 2001 are written to print files CMPRT01 (list of log records) and CMPRT02 (detailed log records information).

Sample Batch Job 3 for Mainframes - Reading Log Records from Work File:

```
//DBA       JOB DBA,CLASS=K,MSGCLASS=X
//**
//** READ LOGGING OF MAINTENANCE DATA FROM WORK FILE 5
//** INTO LOG FILE
//**
//NSCnnBAT EXEC PGM=NATBATnn,REGION=2400K,
// PARM=('IM=D,FNAT=(22,210),INTENS=1,FSEC=(22,240),',
//       'MT=0,MAXCL=0,MADIO=0,AUTO=OFF,WORK=((5),OPEN=ACC)')
//STEPLIB DD   DSN=PRODNAT.LOAD,DISP=SHR
//DDCARD   DD  DISP=SHR,DSN=PRD.NATnn.JOBS(ADADB22)
//CMPRINT  DD  SYSOUT=X
//CMWKF05  DD  DSN=NSC.LOG.WKF05,DISP=(SHR)
//CMSYNIN   DD *
SYSSEC,DBA,password
LOGFILE
22,241
RA,US,,2001-07-01,2001-07-25
.
FIN
/*
//*
```

In the above example, the log records of all user security profiles modified between 1st and 25th of July 2001 are read from Work File 5 and thus restored on the log file.

See also the section Natural Security In Batch Mode.

List Last Logon Records

Note:
This function is independent of the logging of maintenance functions. Internally, however, it uses the same log file.

This function evaluates the logon records that have been written by Natural Security (see Functions of Logon Records Processing above). It allows you to ascertain:

- when each user logged on last,
- which users have not logged on within the last *n* days.

When you invoke the function, a window will be displayed in which you enter a number of days*:*

- If you enter a "0", you will get a list of logon records showing the latest logon record written for each user.
- If you enter any other value *n*, you will get a list of logon records of those users who have not logged on in the last *n* days, showing for each of those users the last logon record written before the specified time interval.

The logon records are listed in chronological order.

Note:
For this function, the fields "Object Type", "Start Value" and "Date from/to" on the menu have no effect.

Definition of System File Access

This function is not available on mainframe computers.

This function allows you to control the access to the Natural system files which are defined in the Natural configuration file NATCONF.CFG.

How to Define the System File Access

On the Main Menu, you select "Administrator Services". The Administrator Services Menu will be displayed.

> **Note:**
> Access to Administrator Services may be restricted; see Access to Administrator Services above.

On the Administrator Services Menu 2, you select "Definition of system file access". A list of all system files defined in the Natural configuration file NATCONF.CFG will be displayed.

The list can be scrolled as described in the section Finding Your Way In Natural Security.

For each system file, the DBID, the FNR and the "Access" status are displayed.

You can set the Access to one of the following:

Ma	**Maintain** - The system file is not protected; it can be accessed by any user (this is the default).
No	**No access** - The system file is protected; it can only be accessed by users who are linked to it.

To change the status of a system file, either you overwrite the value of the Access field, or you enter the value in the Code field (see below).

When you change it back to "Ma", all links to the file are automatically deleted.

The following functions are available for system files (possible code abbreviations are underlined):

Code	**Function**
NO	**Set access "No"** - This function changes the Access status of the system file to "No".
MA	**Set access "Ma"** - This function resets the Access status of the system file to "Ma", and at the same time deletes all links to the system file.
LU	**Link user** - This function is used to link users to a protected system (as described below).
PA	**Display path** - This function displays the path name of the system file as defined in NATCONV.CFG. To display the path name, you can also place the cursor in the line containing the desired system file, and then press PF5.

To invoke a specific function for a system file, mark the file with the appropriate function code in column "Co".

You may select various system files for various functions at the same time; that is, you can mark several files on the screen with a function code. For each file marked, the selected functions will then be executed one after another.

Linking Users to a Protected System File

To allow a user access to a protected system file, a *link* has to be established between the user and the system file.

Only users of types GROUP, ADMINISTRATOR and PERSON can be linked to a system file. Users of types ADMINISTRATOR and PERSON can be linked to a system file either directly or via a GROUP. Users of types MEMBER and TERMINAL can be linked to a system file only via a GROUP; that is, they must be assigned to a GROUP, and the GROUP be linked to the system file.

On the system file selection list, you mark the file to which you wish to link users with code "LU".

A window will be displayed in which you can enter a start value for the list of users to be displayed. Then, the Link Users To System File selection list will be displayed, showing the list of users.

By default, the list contains only users of type GROUP. To switch between a list of GROUPs and a list of all three user types, you press PF5.

The list can be scrolled as described in the section Finding Your Way In Natural Security.

On the list, you mark the users you wish to be linked to the system file.

In the "Co" column, you may mark each user with one of the following function codes (possible code abbreviations are underlined):

Code	Function
LK	**Link** - The user may access the system file.
CL	**Cancel** - An existing link will be cancelled.
DI	**Display user** - The security profile of the user will be displayed.

You can mark one or more users on the screen with a function code. For each user marked, the selected functions will then be executed one after another. When processing is completed, a message will be displayed stating the link situation now in effect for each user.